

Flowmon and Prolion: Enhancing Data Security

Proactively Detecting Ransomware Threats

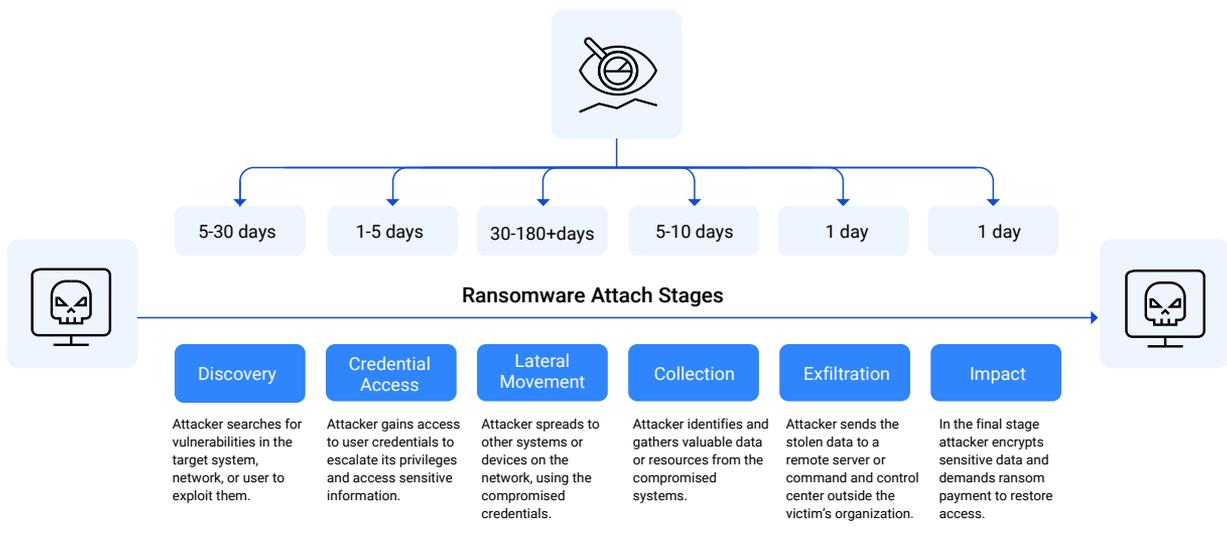
DATA SHEET

Protecting data is crucial. In a recent study, organizations worldwide reported nearly half a billion ransomware attempts—all reported within a 12 month period – which equates to 15 attacks every second. This highlights the importance of Dell Technologies providing its Prolion and Storage customers with proactive solutions to detect, protect against, and recover from such threats.

Dell Technologies offers a suite of tools that monitor activity at the data layer by analyzing audit logs that track actions such as file access (open, close, delete, rename), as well as when and where these occur on storage platforms like PowerScale, PowerStore, and Unity. However, by this stage, the data has already been exposed to a significant ransomware risk. This approach:

- Is reactive, akin to firefighting,
- Occurs during the “Collection” phase of an attack (as shown in the diagram),
- Focuses on minimizing damage and ensuring the availability of a valid copy of the data for recovery

Dell Technologies now offers its storage customers a more proactive solution through the integration of Prolion CryptoSpike. This solution enables the detection of suspicious activity during the “Discovery” phase of an attack—long before malicious actors gain access to sensitive data.



Detect a ransomware attack at every stage - powered by Progress

